

WHAT IS CLAIMED IS

1. A system for facilitating wireless data communication, comprising:

an operations center configured to implement access control rules within an

emergency zone;

an access device configured to provide preferential access to a network to emergency
devices over non-emergency devices within the emergency zone based on the access control
rules.
2. The system of claim 1, wherein the operations center is configured to
transmit the access control rules to the access device.
3. The system of claim 1, wherein the access control rules reside in a memory
of the access device, and

wherein the operations center is configured to send an emergency message that
activates the access control rules.
4. The system of claim 1, wherein the access device includes a wireless access
point configured to wirelessly communicate with the non-emergency devices and the emergency
devices.
5. The system of claim 4, wherein the wireless access point includes:

a processor configured to filter wireless data based on the access control rules, and
a wireless transceiver connected to the processor and configured to send and receive
wireless data.

6. The system of claim 1, further comprising:

at least one wireless access point configured to wirelessly communicate with the non-
emergency devices and the emergency devices,

wherein the access device includes a gateway connected between the at least one
wireless access point and the network and configured to control access to the network by data
from the at least one wireless access point.

7. A method, comprising:

determining a need for an emergency zone in which wireless data access is to be
restricted to emergency devices;

associating one or more access devices with the emergency zone; and

sending an emergency message to the one or more access devices for wireless data
access within the emergency zone to be restricted to the emergency devices.

8. The method of claim 7, wherein the associating includes:

designating, by a network operator, a set of access devices as corresponding to the
emergency zone.

9. The method of claim 7, wherein the emergency message includes access control rules for storage in and implementation by the one or more access devices.

10. The method of claim 7, wherein the emergency message includes one or more commands to activate access control rules that reside in the one or more access devices.

11. The method of claim 7, sending an emergency message includes:
sending the emergency message to one or more wireless access points that wirelessly communicate with the emergency devices.

12. The method of claim 7, sending an emergency message includes:
sending the emergency message to one or more gateway devices that control data traffic from one or more wireless access points.

13. A method, comprising:
validating an emergency message;
implementing access control rules based on the emergency message; and
controlling access by wireless data devices to give preference to emergency devices based on the access control rules.

14. The method of claim 13, wherein the validating includes:

cryptographically validating the emergency message using an emergency cryptographic key.

15. The method of claim 13, wherein the implementing includes:
extracting the access control rules from the emergency message, and
installing the access control rules.

16. The method of claim 13, wherein the implementing includes:
providing parameters from the emergency message to installed access control rules.

17. The method of claim 13, wherein the controlling access includes:
limiting wireless data access to emergency devices based on a set of addresses.

18. The method of claim 17, wherein the set of addresses includes media access control (MAC) addresses.

19. The method of claim 17, wherein the set of addresses includes Internet protocol (IP) addresses.

20. The method of claim 17, wherein the limiting wireless data access includes selectively refusing to complete a communication protocol handshake.

21. The method of claim 13, wherein the controlling access includes:
limiting wireless data access to emergency devices based on authentication
information provided by the emergency devices.

22. A computer-readable medium that stores instructions executable by one or
more processors to perform a method for controlling data access in a wireless network,
comprising:

instructions for differentiating between emergency devices and non-emergency
devices;

instructions for allowing wireless data access to the emergency devices in an
emergency zone; and

instructions for limiting wireless data access to the non-emergency devices in the
emergency zone.

23. The computer-readable medium of claim 22, wherein the instructions for differentiating include:

instructions for classifying data from a wireless device based on media access control (MAC) addresses, Internet protocol (IP) addresses, or authentication information.

24. The computer-readable medium of claim 22, wherein the instructions for limiting wireless data access include:

instructions for denying wireless data access to the non-emergency devices in the emergency zone.

25. A system for providing emergency wireless data access in a network, comprising:

means for receiving communication requests that were initiated by wireless devices;

means for storing access control rules for controlling wireless data access during an emergency; and

means for selectively processing the communication requests in accordance with the access control rules during the emergency.

26. The system of claim 25, wherein the means for receiving includes:

means for receiving wireless data from the wireless devices.

27. A method for controlling data access in a wireless network, comprising:

differentiating between emergency devices and non-emergency devices during an emergency;

allowing wireless data access to the emergency devices in an emergency zone during the emergency; and

limiting wireless data access to the non-emergency devices in the emergency zone during the emergency.